

✓ CZY JESTEŚ GOTOWY DO RODO?

4 TECHNICZNE ZABEZPIECZENIE DANYCH

- Czy spółka zweryfikowała system informatyczny w ramach którego przetwarza dane osobowe?
- Czy spółka ustaliła, czy przechowuje dane na własnych serwerach, czy też korzysta w tym zakresie z usług hostingowych?
- Czy spółka dokonała analizy, w jaki sposób przechowywane przez spółkę dane są chronione przed nieautoryzowanym dostępem osób trzecich, w tym zarówno z zewnątrz, jak i ze strony pracowników i współpracowników?
- Czy spółka dokonała analizy, w jaki sposób przechowywane przez spółkę dane są chronione przed przypadkowym zniszczeniem, usunięciem, zniekształceniem?
- Czy spółka zbadała jakie zabezpieczenia informatyczne stosuje przed zagrożeniem typu wirusy, złośliwe oprogramowanie, trojany, ransomware, etc?
- Czy spółka zweryfikowała stosowane rozwiązania kontroli dostępu do zasobów obejmujących dane osobowe w zakresie używanych systemów informatycznych, w szczególności, czy spółka stosuje ograniczenia dostępu poszczególnych pracowników do poszczególnych zasobów, w zależności od treści udzielonego tym pracownikom upoważnienia w zakresie przetwarzania danych osobowych, ograniczenia dostępu w zakresie poziomu dostępu do danych, lub logowania dostępu poszczególnych pracowników posiadających upoważnienie w zakresie przetwarzania danych osobowych do poszczególnych zasobów?
- Czy spółka zbadała w jaki sposób wykorzystywany przez spółkę system teleinformatyczny jest zabezpieczony w sposób fizyczny przed dostępem nieuprawnionych osób, w szczególności, czy spółka korzysta z zamkniętych dedykowanych pomieszczeń mieszczących serwery, w jaki sposób stacje robocze (np. laptopy), na których przetwarzane są dane osobowe zabezpieczone są przed nieautoryzowanym dostępem osób nieuprawnionych lub kradzieżą (np. blokady Kensington Lock)?
- Czy spółka zweryfikowała w jaki sposób chroniona jest zawartość wykorzystywanych przez spółkę komputerów i urządzeń mobilnych, na których przetwarzane są dane, w szczególności czy stosowane są hasła dostępu z kryteriami siły haseł, czy system wymusza okresową zmianę hasła, kody PIN, czy urządzenia są szyfrowane, czy porty USB w urządzeniach, w których przetwarzane są dane zostały zablokowane w sposób uniemożliwiający podłączenie do nich zewnętrznych nośników pamięci?
- Czy spółka dokonała weryfikacji sposobu zasilania infrastruktury technicznej?
- Czy spółka dokonała weryfikacji, czy używane systemy teleinformatyczne udostępniające dane wyposażone są w źródło podtrzymania zasilania?
- Czy spółka zbadała, czy wykonuje kopie bezpieczeństwa danych z serwerów i innych systemów udostępniających dane?
- Czy spółka zbadała, w jaki sposób zabezpieczone są skrzynki e-mailowe wykorzystywane przez spółkę?
- Czy spółka zbadała, czy możliwy jest dostęp do zasobów obejmujących dane osobowe za pośrednictwem nieautoryzowanych urządzeń?

5 DOKUMENTACJA I WEWNĘTRZNA ORGANIZACJA PROCESU PRZETWARZANIA DANYCH

- Czy na podstawie obowiązujących przepisów ustawy o ochronie danych osobowych spółka zgłosiła zbiory danych osobowych Generalnemu Inspektorowi Danych Osobowych?
- Czy spółka zbadała, w jaki sposób zabezpieczane są dane osobowe przechowywane w tradycyjnej formie papierowej przed nieautoryzowanym dostępem osób trzecich?
- Czy spółka zweryfikowała, czy zobligowana jest do wykonania oceny skutków dla ochrony danych (ang. Data Protection Impact Assessment – DPIA), a jeśli tak, to czy spółka przygotowała DPIA?
- Czy spółka zweryfikowała konieczność konsultacji z organem nadzorczym?
- Czy spółka zweryfikowała konieczność powołania Inspektora Danych Osobowych?
- Czy spółka opracowała rejestr czynności przetwarzania danych?
- Czy spółka dokonała weryfikacji, czy przetwarza dane osobowe na zlecenie innego podmiotu, który decyduje o celach i sposobach przetwarzania, a jeżeli tak, to czy spółka opracowała rejestr kategorii czynności przetwarzania w imieniu administratora danych?
- Czy spółka opracowała rejestr naruszeń ochrony danych osobowych?
- Czy spółka opracowała wzór zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych?
- Czy spółka dokonała analizy, czy jakiegokolwiek osoby wyznaczone przez spółkę (w formie pisemnej) jako odpowiedzialne za ochronę danych, posiadają wiedzę na temat obowiązków związanych z ochroną danych osobowych?
- Czy spółka zweryfikowała upoważnienia do przetwarzania danych osobowych udzielone przez spółkę swoim pracownikom lub współpracownikom?
- Czy spółka wdrożyła procedury ochrony danych osobowych i przeszkoliła w tym zakresie swoich pracowników i współpracowników?
- Czy spółka zweryfikowała, czy inne podmioty (np. z grupy kapitałowej do której należy spółka) współstalają ze spółką cele i sposoby przetwarzania danych?
- Czy spółka zweryfikowała, czy inne podmioty (np. z grupy kapitałowej do której należy spółka) decydują o celach i sposobach przetwarzania przez spółkę danych osobowych wraz z innym podmiotem?

